АНО ДПО «Институт профессионального кадровика»

127410, г.Москва, вн.тер. г.муниципальный округ Отрадное, Ш. Алтуфьевское, Д. 41а, стр. 1

УТВЕРЖДАЮ
Директор _____ Мащенко М.С.
«17» июля 2026

УЧЕБНЫЙ ПЛАН

программы повышения квалификации

«Специалист по защите персональных данных: пошаговое построение и аудит системы защиты»

Обязательный курс для специалистов по информационной безопасности, управлению персоналом, кадровому делопроизводству, руководителей структурных подразделений, юристов и иных лиц, ответственных за организацию работы с персональными данными.

Цель обучения: Формирование у слушателей системного алгоритма действий по построению, проверке и оптимизации Системы защиты персональных данных (СЗПД) в организации. Профессиональное обучение лиц в целях совершенствования навыков для выполнения требований ст. 18.1. Федерального закона «О персональных данных» и успешного прохождения проверок Роскомнадзора.

Категория слушателей: Лица, ответственные за организацию работы с персональными данными и допущенные к работе с ними (управление персоналом, ИТ-специалисты, юристы, руководители подразделений, специалисты по внутренней безопасности и аудиту).

Форма: заочная.

Срок освоения программы: 2 месяца (60 календарных дней)

Продолжительность: 72 ак. часа.

Документ по итогам: удостоверение о повышении квалификации установленного образца.

Задачи обучения (Пошаговый алгоритм):

- Шаг 1 (Аудит): Провести инвентаризацию данных и картирование бизнес-процессов.
- Шаг 2 (Фундамент): Назначить ответственных и разработать систему локальных нормативных актов (ЛНА).
- Шаг 3 (Легитимизация): Выстроить корректный механизм получения согласий и правовых оснований.
- Шаг 4 (Регулятор): Правильно уведомить Роскомнадзор о начале и изменениях в обработке.

- Шаг 5 (Защита): Внедрить необходимые организационные и технические меры защиты (для ИС и бумажных носителей).
- Шаг 6 (Жизненный цикл): Настроить процессы хранения, ответов на запросы и уничтожения данных.
- Шаг 7 (Контроль): Подготовиться к инспекционной проверке Роскомнадзора и минимизировать риски штрафов.

ПРОГРАММА ОБУЧЕНИЯ

№ п/п	Наименование модулей (шагов) и тем	Всего часов
1.	МОДУЛЬ 1. Аудит и фундамент: Анализ процессов и категорирование данных	8
1.1.	Нормативно-правовая база: актуальные требования, изменения законодательства и тренды.	2
1.2.	Терминология и субъекты ПДн: идентификация потоков данных в организации.	2
1.3.	Инвентаризация ПДн: категории, специальные и биометрические данные, особенности их обработки.	2
1.4.	Картирование бизнес-процессов: как выявить все места сбора и обработки ПДн в компании.	2
2.	МОДУЛЬ 2. Организационный каркас: Ответственные лица и разработка ЛНА	12
2.1.	Назначение ответственных лиц за организацию и обработку ПДн. Организация их инструктажа.	2
2.2.	Архитектура системы ЛНА по защите ПДн: от Политики до локальных инструкций и регламентов.	2
2.3.	Работа с кадровыми документами: как проверить соблюдение требований и избежать типичных нарушений.	4
2.4.	Регулирование передачи ПДн третьим лицам: договоры, поручения на обработку, согласования.	2
2.5.	Внутренний контроль и аудит: построение системы регулярного мониторинга соблюдения ЛНА.	2
3.	МОДУЛЬ 3. Легитимизация обработки: Согласия и правовые основания	10
3.1.	Правовые основания обработки: какие данные и в каких случаях можно обрабатывать без согласия.	2
3.2.	Требования к форме и содержанию согласия на обработку ПДн (сотрудники, клиенты, посетители).	4
3.3.	Согласие на распространение и передачу ПДн третьим лицам: специфика и механизмы реализации.	2
3.4.	Механизмы получения, учета, хранения и отзыва согласий субъектов ПДн.	2
4.	МОДУЛЬ 4. Взаимодействие с регулятором: Уведомление Роскомнадзора	6
4.1.	Уведомление о начале обработки ПДн: порядок, сроки, заполнение форм.	2
4.2.	Уведомление в случае изменения целей, состава данных или прекращения обработки ПДн.	2
4.3.	Специфика уведомления и согласования при трансграничной передаче ПДн.	2
5.	МОДУЛЬ 5. Защита данных: Организационные и технические меры	14

№ п/п	Наименование модулей (шагов) и тем	Всего часов
5.1.	Моделирование угроз безопасности ПДн: определение актуальных угроз для конкретной организации.	2
5.2.	Защита ПДн в информационных системах (ИС): определение уровней защищенности и выбор мер.	4
5.3.	Защита ПДн без применения ИС (бумажные носители): требования к сейфам, шкафам, журналам.	4
5.4.	Обязанности должностных лиц при работе в ИС и с бумажными носителями (режим конфиденциальности).	2
5.5.	Алгоритм определения перечня необходимых технических и организационных мер защиты.	2
6.	МОДУЛЬ 6. Жизненный цикл ПДн: От запросов до уничтожения	10
6.1.	Алгоритмы ответов на запросы субъектов ПДн и Роскомнадзора: сроки, форматы, риски.	4
6.2.	Порядок и сроки хранения ПДн: установление политики удержания данных (Retention) в компании.	2
6.3.	Регламентация и порядок уничтожения ПДн (истечение срока обработки, отзыв согласия, ликвидация).	4
7.	МОДУЛЬ 7. Контроль и защита: Подготовка к проверкам и ответственность	12
7.1.	Виды проверок Роскомнадзора: нормативное регулирование, регулярность, полномочия инспекторов.	2
7.2.	Чек-листы самопроверки: пошаговая подготовка к инспекционной проверке (аудит готовности).	6
7.3.	Риски и ответственность организации и должностных лиц за нарушения законодательства о ПДн.	2
	ИТОГО:	72 ак.часа